INFORMATION AND CONTROL 20, 125–134 (1972)

On the Automorphism Groups of Periodic Automata

BRUCE H. BARNES

Department of Computer Science, The Pennsylvania State University, University Park, Pennsylvania 16802

The purpose of this investigation is to determine how the structure of a strongly connected strictly periodic automaton is reflected in the structure of its automorphism group. It is shown that the group of automorphisms of an automaton of this type can be represented as the direct product of two normal subgroups. The automorphism group for the special class of equipotent automata is also investigated. It is also shown that the group of automorphisms can be useful in determining decompositions of automata into smaller automata.

INTRODUCTION

The concept of a periodic automaton was introduced by Gill (1963). The relationships between the periodicity of an automaton and its structure has been investigated by Gill and Flexer (1967), Grzymalla–Busse (1969a), and Guha and Yeh. Grzymalla–Busse (1969) observed that the periodicity of an automaton is reflected in its algebraic structure. He investigated the structure preserving transformations on the class of strongly connected strictly periodic equipotent automata, which are a type of time-varying automata. In particular, he defined a polyadic automorphism and showed that the set of all polyadic automorphisms formed a polyadic group. Using this polyadic group, he was able to demonstrate some of the special properties of these transformations and to show that most of the standard results concerning the automorphism groups of automata as found in the papers of Weeg, Fleck and the author had an equivalent formulation in polyadic groups. One of the purposes of this investigation is to investigate the groups of automorphisms for the class of strongly connected strictly periodic automata. In particular it will be shown that the group of all automorphisms of an automaton of this type can be represented as the direct product of two special subgroups of automorphisms. Another is to show that for the same class as investigated by Grzymalla–Busse the group of automorphisms does a better job of capturing the structure of an automaton than polyadic automorphisms. It will also be

643/20/2-3

shown that the group of automorphisms is useful in determining decompositions into simpler automata.

Definitions and Preliminaries

In this section some of the necessary definitions, concepts and theorems of time-varying automata and the group of automorphisms of finite automata will be presented. For a complete discussion of these topics one should consult Gill (1963) and Grzymalla–Busse (1969).

Definition 1. A *time-varying automaton* is a triple (S, Σ, M), where S is an infinite sequence of sets of states

$$S_0, S_1, \ldots, S_i, \ldots, S_t = \{s_0^{(t)}, s_1^{(t)}, \ldots, s_{m_t-1}^{(t)}\};$$

Σ is a fixed nonempty set of input symbols; $\Sigma = \{\sigma_0, \sigma_1, \ldots, \sigma_n\}$; M is an infinite sequence of next-state functions $M_0, M_1, \ldots, M_t, \ldots$, and M_t has the domain $S_t \times \Sigma$ and the range S_{t+1} for all $t = 0, 1, \ldots$.

The sequential property is also assumed. That is,

$$\begin{aligned} M_t(s, \sigma_0\sigma_1 \cdots \sigma_{k-1}) &= M_{t+1}(M_t(s, \sigma_0), \sigma_1 \cdots \sigma_{k-1}) \\ &= \cdots = M_{t+k-1}(\ldots M_{t+1}(M_t s_0, \sigma_0), \ldots, \sigma_{k-1}). \end{aligned}$$

The set of all finite sequences of elements of Σ is denoted by Σ^*.

Definition 2. A time-varying automaton in which for $t = 0, 1, \ldots$ the cardinality of each state set S_t does not exceed a fixed finite bound is called a *bounded automaton.*

Definition 3. A bounded automaton for which there exist two integers $T \geqslant 1$ and $\tau \geqslant 0$ such that for each $t > \tau$ the state set S_t is equal to the state set S_{T+t} and the function M_t is equal to the function M_{T+t}, is a *periodic automaton* where T is the period and τ the transient duration of the periodic automaton.

We are now in a position to define the class of time-varying automata that we will be primarily concerned with.

Definition 4. A periodic automaton for which the transient duration τ is equal to zero is called a *strictly periodic automaton.*

Note that if the period T of a strictly periodic automaton is equal to 1, then it is finite automaton in the usual sense. Likewise, corresponding to each periodic automaton is a finite automaton called the fixed analog, which is in a sense identical to the periodic automaton.

DEFINITION 5. Let $A = (S, \Sigma, M)$ be a periodic automaton with period T and transient duration τ. The *fixed analog* A^* of A is the finite automaton $A^* = (S^*, \Sigma, M^*)$, where $S^* = \bigcup_{i=0}^{t+T-1} S_i$, and M^* is a mapping of $S \times \Sigma$ into S defined as follows:
$M^*(s, \sigma) = M_t(s, \sigma)$ for all $s \in S_t$, all $\sigma \in \Sigma$ and for $t = 0, 1,..., \tau + T - 1$.

DEFINITION 6 (Grzymalla-Busse, 1969). A strictly periodic automaton $A = (S, \Sigma, M)$ with a period T such that for all $s_i \in S_i$, $s_j \in S_{i+1}$ and $i = 0, 1,..., T - 1$, there is an $x \in \Sigma^*$ such that $M_t(s_i, x) = s_j$ is said to be *strongly connected.*

It can be readily seen that a strictly periodic automaton A is strongly connected if and only if its fixed analog A^* is strongly connected in the usual sense. In the remainder of the investigation we will only be concerned with strongly connected strictly periodic automata.

DEFINITION 7. Let $A = (S, \Sigma, M)$ be a strictly periodic automaton and A^* its fixed analog. A one-to-one mapping h of S onto S such that $h(M^*(s, x)) = (M^*(h(s)x)$ for all $s \in S$ and all $x \in \Sigma$ is called an automorphism of A.

It has been shown by Fleck (1962) that the set of all automorphisms of A forms a group, denoted by $G(A)$. It is our purpose to show how the periodic nature of a strictly periodic automaton affects the structure of its automorphism group. We will make considerable use of the concepts of partition with substitution property and full subautomata.

DEFINITION 8. Let $A = (S, \Sigma, M)$ be a finite automaton and π a partition on S. π has the *substitution property,* S.P., if whenever $s_i \equiv s_j \pmod{\pi}$ implies $M(s_i, x) \equiv M(s_j, x) \pmod{\pi}$ for all $x \in \Sigma$. For a discussion of partitions with the substitution property consult Hartmanis and Stearns (1966).

Corresponding to each strictly periodic automaton $A = (S, \Sigma, M)$ is a partition Π with S.P. Π is defined by: two states are associated if and only if they are in the state set S_t. That is, $s_i \equiv s_j \pmod{\Pi}$ if and only if s_i and s_j are both in S_t. The state sets S_t, $t = 0, 1,..., T - 1$, will be called the components of A and this particular partition the component partition.

DEFINITION 9. Let $A = (S, \Sigma, M)$ be a finite automaton. If S' is a subset of S, Σ' a subsemigroup of Σ^* such that $M(s, x) \in S'$ for $s \in S'$ and all

$x \in \Sigma'$, then $A' = (S', \Sigma', M')$ is called a *subautomaton* of A, where M' is the restriction of M to $S' \times \Sigma'$.

It should be noted that this definition differs from that of other authors in that they require that $\Sigma' = \Sigma$.

DEFINITION 10. Let $A = (S, \Sigma, M)$ be a finite automaton. A subautomaton $A' = (S', \Sigma', M')$ with the property that if $x \in \Sigma^*$ and $M(s_i, x) \in S'$ for at least one $s_i \in S'$ then $x \in \Sigma'$, is called a *full subautomaton.*

Each component in a strictly periodic automaton $A = (S, \Sigma, M)$ is the state set for a full subautomaton. The input set consists of all input sequences of length mT, where m is a positive integer and T is the period of A. This is because of the periodic nature of A implies s_i and $M(s_i, x)$ are in the same component of A if and only if x is of length mT.

Following Weeg (1965) we will use the notation T_{ij} to denote the set of all $x \in \Sigma^*$ such that $M(s_i, x) = s_j$. Note that if $x \in T_{ii}$, then its length is a multiple of the period T. The author (1970) has given the following necessary and sufficient conditions for a strongly connected finite automaton to have a group or subgroup of automorphisms.

THEOREM 1. *Let $A = (S, \Sigma, M)$ be a strongly connected finite automaton with n states. A has a subgroup of automorphisms, H, of order m if and only if there exists a partition π on S with m states in each block such that π has the substitution property and $T_{ii} = T_{jj}$ whenever s_i and s_j are in the same block of π.*

THEOREM 2. *Let $A = (S, \Sigma, M)$ be a strongly connected finite automaton. The group of all automorphisms of A, $G(A)$, is of order m if and only if there exists a partition π on the state set S such that*

(1) *each block of π has m states,*
(2) *if $s_i \equiv s_j \pmod{\pi}$, then $T_{ii} = T_{jj}$,*
(3) *π is the largest partition on S satisfying* (2).

STRICTLY PERIODIC AUTOMATA

In this section the structure of the automorphism group of a strictly periodic automaton will be investigated. It will be shown that for this class of automata the group of automorphisms, $G(A)$, can be represented as a direct product of subgroups.

DEFINITION 11. A *component automorphism* of a strictly periodic automaton $A = (S, \Sigma, M)$ with period T is a mapping $g = (g_0, g_1, \ldots, g_{T-1})$, where each g_i is a one-to-one mapping of S_i onto S_i such that $M(g(s), x) = g(M(s, x))$ for all $s \in S$ and all $x \in \Sigma$.

It can readily be seen that the set of all component automorphisms form a group, that will be denoted by $C(A)$. Since any component automorphism also is a one-to-one mapping of S onto S, it is an automorphism of A and consequently $C(A)$ is a subgroup of $G(A)$. We will, in fact, show that if A is strongly connected, then $C(A)$ is a normal subgroup. For this purpose and for our later investigations the following lemma will prove useful.

LEMMA 1. *Let $A = (S, \Sigma, M)$ be a strongly connected strictly periodic automaton with period T and let h be an automorphism of A. If s_i and s_j are both in the same component of S, then so are $h(s_i)$ and $h(s_j)$ both in a component of S.*

Proof. Since A is strongly connected, there is some $z \in \Sigma^*$ such that $M(s_i, z) = s_j$. Note that the length of z is a multiple of T. Consider $h(s_j) = h(M(s_i, z)) = M(h(s_i), z)$. Since z is a multiple of length T, $M(h(s_i)z)$ and $h(s_i)$ are in the same S_i, thus $h(s_j)$ is also in the same component as $h(s_i)$.

THEOREM 3. *Let $A = (S, \Sigma, M)$ be a strongly connected strictly periodic automaton. Then $C(A)$ is a normal subgroup of $G(A)$.*

Proof. Let g be any component automorphism, h any automorphism and s_i a state in component S_j. Consider the mapping $h^{-1}gh$. The automorphism h will map the state $s_i \in S_j$ into some state say s_k in component S_l; since $g \in C(A)$, $g(s_k)$ is also in S_l. Since $h^{-1}(s_k) = s_i \in S_j$; by Lemma 1, $g(s_k) \in S_j$. Thus $h^{-1}gh \in C(A)$ and consequently $C(A)$ is a normal subgroup of $G(A)$.

The subgroup of component automorphisms contains all the automorphisms which map the components onto themselves. There might be, however, automorphisms which map the states in one component onto the states in a different component. It will be shown that the structure of this type of automorphism is captured by a cyclic subgroup of the automorphism group.

THEOREM 4. *Let $A = (S, \Sigma, M)$ be a strongly connected periodic automaton with period T. Then $G(A)/C(A)$ is a cyclic group whose order divides T and is isomorphic to a normal subgroup of $G(A)$.*

Proof. Let the components of A be $S_0, S_1, \ldots, S_{T-1}$. Let h be a noncomponent automorphism such that $h(S_0) = S_i$, and $i \neq 0$, but there does not exist a noncomponent automorphism h' such that $h'(S_0) = S_j$ and

$0 < j < i$. That is that h is an automorphism such that its image of S_0 is "closest" to S_0. From the definition of automorphism and the periodic structure of the automaton A, it follows that $h^2(S_0) = S_{2i(\bmod T)}$. There cannot be an m such that $h^m(S_0) = S_j$, $0 < j < i$, otherwise, there would be an automorphism with this property. Consequently, i divides T. Let k be any other automorphism which maps S_0 onto S_i. That is $h(s_{00}) = s_{i0}$ and $k(s_{00}) = s_{i1}$, where $s_{00} \in S_0$ and s_{i0}, $s_{i1} \in S_i$. There is some power of h, say m, such that h^m is the identity. Thus $h^{m-1}k(s_{i0}) = s_{i1}$ and $h^{m-1}k \in C(A)$. Thus h and k are in the same coset of $G(A)/C(A)$. By a similar argument it can be shown that if $G(A)/C(A)$ is not cyclic, then there would be some automorphism k such that $k(S_0) = S_j$, where $0 < j < i$. This would be contrary to the hypothesis. Thus, $G(A)/C(A)$ is cyclic.

Let H be the set of all automorphisms that map S_0 onto S_i and m the order of the cyclic group $G(A)/C(A)$. If $m = 1$ then all automorphisms are component automorphisms and H is empty. Assume H is not empty and consider the set $H^m = \{h^m / h \in H\}$. This must be equal to $C(A)$. Thus, there is some element $h_1 \in H$ such that $h_1{}^m = I$. This element is the generator of a subgroup of $G(A)$ which is isomorphic to $G(A)/C(A)$. An argument similar to that of Theorem 3 will show that the subgroup generated by h_1 is a normal subgroup of $G(A)$.

THEOREM 5. *Let $A = (S, \Sigma, M)$ be a periodic automaton with period T. Then $G(A)$ is isomorphic to a direct product of two groups, one of which is isomorphic to the component subgroup and the other is a cyclic group whose order divides T.*

Proof. By Theorem 3 and 4 both $C(A)$ and $G(A)/C(A)$ are isomorphic to normal subgroups. Clearly

$$C(A) \cap G(A)/C(A) = I \qquad \text{and} \qquad C(A) \cup G(A)/C(A) = G(A).$$

Thus the necessary conditions for a finite group to be isomorphic to a direct product of normal subgroup are satisfied. For a discussion of direct products of groups see for example Hall (1959).

EQUIPOTENT PERIODIC AUTOMATA

A very interesting special class of periodic automata is the class where each component has the same number of states. The elements of this class are called equipotent automata and are the type investigated by Grzymalla–Busse (1969).

In this section the relationship between equipotent automata and transitive automata, as studied by Weeg (1965) and the author (1965, 1970) will be shown.

DEFINITION 12. Let $A = (S, \Sigma, M)$ be a strongly connected strictly periodic automaton with period T. If $| S_i | = | S_j |$ for all $0 \leqslant i \leqslant j \leqslant T - 1$, then A is an *equipotent automaton.*

DEFINITION 13. Let $A = (S, \Sigma, M)$ be a strongly connected finite automaton with n states. A is said to be a *transitive automaton* if and only if the order of $G(A)$ equals n.

When A is not an equipotent automaton, then A is not transitive. This can be seen from the following theorem.

THEOREM 6. *Let $A = (S, \Sigma, M)$ be a strongly connected strictly periodic automaton. There is an automorphism h such that $h(s_i) = s_j$ only if $| S_i | = | S_j |$, where $s_i \in S_i$ and $s_j \in S_j$.*

Proof. Suppose that was not the case and $| S_i | > | S_j |$. Then there would be some state say $s_k \in S_i$ such that $h(s_k) \notin S_j$. Since A is strongly connected, there is a tape $x \in \Sigma^*$ such that $M(s_i, x) = s_k$. Consider $M(h(s_i), x) = M(s_j, x) \in S_j$, but $h(M(s_i, x)) = h(s_k) \notin S_j$. Thus, $| S_i | = | S_j |$.

COROLLARY 1. *Let $A = (S, \Sigma, M)$ be a strongly connected strictly periodic automaton. If A is a transitive, then A is equipotent.*

This follows directly from the previous theorem and the definition of equipotent.

If the automaton is not equipotent, there cannot be any automorphism which maps S_0 onto S_1. Otherwise some power of this automorphism would map S_0 to each other component. Such automorphisms, called periodic automorphisms, while nonexistent for nonequipotent automata play a key role in the study of the automorphism group of equipotent automata.

DEFINITION 14. Let $A = (S, \Sigma, M)$ be an equipotent automaton. An automorphism h is said to be a *periodic automorphism* if $h(S_0) = S_1$.

LEMMA 2. *Let $A = (S, \Sigma, M)$ be an automaton with period T, and h a periodic automorphism. Then $h(S_i) = S_{i+1 (\mathrm{mod}\, T)}$.*

This lemma follows directly from the definitions of automorphism, strongly connected, equipotent and Lemma 1.

It should be noted that the $(T-1)$-adic automorphisms of Grzymalla–Busse (1969) are in effect identical to the periodic automorphisms. That is corresponding to each $(T-1)$-adic automorphism is a periodic automorphism and conversely. It should also be noted that he used automorphism or ordinary automorphism in the same sense as component automorphism is used here. In his paper he does not discuss automorphism in the more usual sense.

The following example is useful to show that there can exist automorphisms which are neither periodic or component automorphisms.

EXAMPLE 1. $A = (S, \Sigma, M)$, where $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$; $\Sigma = \{0, 1\}$; M is given by the transition Table I.

TABLE I

Transition Table for the Automaton A

	Input	
State	0	1
1	2	6
2	3	3
3	4	8
4	1	1
5	6	2
6	7	7
7	8	4
8	5	5

The group of automorphisms for the automaton A of Example 1 is the group generated by the permutations $a = (1, 5)(2, 6)(3, 7)(4, 8)$ and $b = (1, 3)(2, 4)(5, 7)(6, 8)$. It is easy to verify that these are automorphisms and that there cannot be any periodic automorphisms.

Let h be a periodic automorphism, then clearly h is of order nT. Thus, $G(A)/C(A)$ is a cyclic group of order T. Thus, if $C(A)$ is transitive on the components of A and A has a periodic automorphism, then $G(A)$ is transitive. This translated to the $(T-1)$-adic automorphisms of Grzymalla–Busse (1969) gives his Theorem 10, which will be stated here in terms of our meaning of automorphism.

THEOREM 7. *Let $A = (S, \Sigma, M)$ be an equipotent automaton, then A is* *transitive if and only if $C(A)$ is transitive on a component and A has a periodic automorphism.*

The sufficiency of the theorem was shown in the preceding remarks. Necessity follows from Lemmas 1 and 2 and Theorem 4.

COROLLARY 2. *Let $A = (S, \Sigma, M)$ be an equipotent automaton, then A is transitive if and only if A has a periodic automorphism and for some $0 \leqslant i \leqslant T - 1$ whenever s_1 and s_k are both in the component S_i, then $T_{11} = T_{kk}$.*

This corollary follows directly from Theorems 1 and 8.

DECOMPOSITION

In this section it will be shown how the automorphism group can be useful in determining decompositions of an automaton into smaller automata.

DEFINITION 13. Let $A = (S, \Sigma, M)$ and $B = (T, \Sigma, N)$ be two automata with the same input set, Σ. The *direct product* of A and B written $A \times B$ is an automaton whose state set is $S \times T$, input set is Σ and next state function is $M \times N$, where $M \times M((s, t), x) = (M(s, x), N(t, x))$.

The following theorem on decomposition is the same as found in Hartmanis and Stearns (1966) except that output are not considered in the case of automata.

THEOREM 8. *Let $A = (S, \Sigma, M)$ be an automaton. Then A is isomorphic to a subautomaton of the direct product of two automata if and only if there are two partitions with the substitution property, Π_1 and Π_2, such that $\Pi_1 \cap \Pi_2 = I$. (That is, each block in Π_1 has only one element in common with any block in Π_2.)*

When an automaton, A, can be represented as the direct product of two automata, it is said to be decomposed into the parallel composition of two automata. Bayer (1966) has pointed out that there is a relation between the subgroups of $G(A)$ and the partitions of A with S.P. A similar approach will be employed here.

THEOREM 9. *Let $A = (S, \Sigma, M)$ be a strongly connected strictly periodic automaton. If $G(A)$ has a nontrivial decomposition into a direct product of normal subgroups, then A has a decomposition into the direct product of automata.*

Proof. Consider the subgroups $C(A)$ and $H = G(A)/C(A)$. By Theorem 4 there is a partition with the substitution property corresponding to each of these subgroups. The blocks of these partitions are effectively the transitivity sets for the subgroups. Since $C(A)$ maps each element into an element in the same component and H maps these elements in another component, no two states are in the same block of the greatest lower bound of the two partitions. Consequently, if $G(A)$ has a nontrivial decomposition, then so does A.

The relationship between the special structure of periodic automata is reflected in the structure of the group of automorphisms of the automata. In particular the cyclic nature of periodic automata is reflected in the necessary cyclic subgroup of $G(A)$. In the decomposition of the automaton, the automaton corresponding to the cyclic subgroup would be in effect a counter.

RECEIVED: November 9, 1970; REVISED: August 18, 1971

REFERENCES

BARNES, B. (1965), Groups of automorphisms and sets of equivalence classes of input for automata, *J. Assoc. Comput. Mach.* **12**, 561–565.

BARNES, B. (1970), On the group of automorphisms of strongly connected automata, *Math. Systems Theory* **4**, 289–294.

BAYER, R. (1966), Automorphism groups and quotients of strongly connected automata and monodic algebras, *Proc. Seventh Ann. Symp. on switching and automata Theory, IEEE Pub.* No. 16-6-40, 282–297.

FLECK, A. C. (1962), Isomorphism groups of automata, *J. Assoc. Comput. Mach.* **9**, 469–476.

FLECK, A. C. (1965), On the automorphism group of an automaton, *J. Assoc. Comput. Mach.* **12**, 566–569.

GILL, A. (1963), Time-varying sequential machines, *J. Franklin Inst.* **276**, 519–539.

GILL, A., AND FLEXER, J. R. (1967), Periodic decomposition of sequential machines, *J. Assoc. Comput. Mach.* **14**, 666–676.

GRZYMALLA-BUSSE, J. W. (1969), Automorphisms of polyadic automata, *J. Assoc. Comput. Mach.* **16**, 208–219.

GRZYMALLA-BUSSE, J. W. (1969a), On the periodic representations and the reducibility of periodic automata, *J. Assoc. Comput. Mach.* **16**, 432–441.

GUHA, R. K., AND YEH, R. T., On periodicity of sequential machines, unpublished.

HALL, M. (1959), "The Theory of Groups," MacMillan Company, New York.

HARTMANIS, J., AND STEARNS, R. E. (1966), "Algebraic Structure of Sequential Machines," Prentice-Hall, Inc., Englewood Cliffs, N. J.

WEEG, G. P. (1962), The structure of an automaton and its operating-preserving transformation group, *J. Assoc. Comput. Mach.* **9**, 345–349.

WEEG, G. P. (1965), The automorphism group of the direct product of strongly related automata, *J. Assoc. Comput. Mach.* **12**, 187–195.